STATEMENT OF WORK (SOW)

Contract Number: **N66001-15-D-0055**
Task Order: **N6600117F6085**
Tracking Number: **7058-H0021**
Task Order Title: **MTC2 SOA Software Application Maintenance Support**
Date: 23 March 2017

1.0 SCOPE:

This is a performance based service acquisition to provide in-house, organic software maintenance engineering, tool enhancements, integration, Information Assurance and documentation revisions for Maritime Tactical Command and Control Service Oriented Architecture (MTC2 SOA) and Program Manager Warfare (PMW) 150 architecture and engineering efforts. The objective of this SOW is to provide support to deployed sites for implementation into MTC2 SOA.

The scope of work will include Command, Control, Communications, Computers, and Intelligence (C4I) software engineering support to Space and Naval Warfare (SPAWAR) Systems Center (SSC) Pacific. This effort will include providing MTC2 SOA software and database integration and support. Support will entail the full range of software development including system requirements, design, implementation, integration, implementation of Software Change Request (SCRs) written against MTC2 SOA software components. Currently, MTC2 SOA software suites are installed at (b)(3); (b)(7)(e)(f) as precursor systems to the Program of Record (POR) release of MTC2. These prototype Command and Control (C2) capabilities require maintenance and system engineering support to maintain the capability and support the transition of capabilities to PMW 150 POR's.

This is a LOE, severable type effort.

1.1 BACKGROUND:

MTC2 SOA is a Science and Technology (S&T) prototype system that is currently fielded operationally at Commander of the U.S. Pacific Fleet (CPF) and the Commander of the U.S. Naval Forces in Europe (C6F), for participation in a variety of C2 activities based on developments. It is a representative system of the next generation Command and Control (C2), software-only solution and is a risk reduction prototype based on Command and Control Rapid Prototype Continuum (C2RPC). MTC2 SOA couples emerging science and technology developments, advanced prototypes and experimentation processes to explore maritime operations center operational level of war needs at fleet commands. It provides planning, execution, monitoring, and assessment.

MTC2 SOA is interoperable with legacy (GCCS-M/J) track managers, sends and receives track data and overlays using Over the Horizon-GOLD (OTH-G) or COP Sync Tools (CST) and can

process data from Navigation Sensor System Interface (NAVSSI), OTH-G, and other Automated Information Systems (AISs), Intelligence Broadcast System (IBS), and Link 16.
MTC2 SOA provides a suite of tools developed to support and coordinate planning, tasking, course of action analyses and execution monitoring displayed in an Ozone Widget Framework (OWF).

2.0 APPLICABLE DOCUMENTS

In the event of a conflict between the text of the statement of work (SOW) and the references cited herein, the text of the SOW shall take precedence. Nothing in the document, however, shall supersede applicable laws and regulations, unless a specific exemption has been obtained. The following documents are for guidance only, except where invoked for a specific section of this SOW.

2.1 Department of Defense Directive 8140.01 (DoDD 8140) CyberSpace Workforce Management; reissues and renumbers DoD Directive (DoDD) 8570.01 (Reference (a)) to update and expand established policies and assigned responsibilities for managing the DoD cyberspace workforce.

a. Department of Defense Directive 8570 (DoDD 8570) Information Assurance Workforce Improvement Program

2.2 Department of the Navy (DON) Information Assurance (IA) Workforce Management Manual (SECNAV M-5239.1)

2.3 Defense Information Systems Agency (DISA) Application Security and Development Security Technical Implementation Guide (STIG)

2.4 OPNAVINST F3300.53C (Series), Navy Antiterrorism Program

2.5 DOD 5220.22-M (Series), National Industrial Security Program Operating Manual (NISPOM)

2.6 National Security Decision Directive 298 (Series), National Operations Security Program (NSDD) 298

2.7 DOD 5205.02E (Series), DOD Operations Security (OPSEC) Program

2.8 OPNAVINST 3432.1A (Series), DON Operations Security

2.9 SPAWARINST 3432.1 (Series), Operations Security Policy

2.10 SSCPACINST 5500.1B, Security Manual (7 JUN 10)

2.11 SSCPACINST 2280.2C and SSC Pacific CMS Training Handbook, dtd April 2012

3.0 BASE PERIOD REQUIREMENTS

3.1 The contractor shall perform analyses and prepare design concepts, concept of operations, functional capabilities descriptions, architecture definitions, designs, technical reports **(CDRL A008)**, and related forms of systems engineering as part of applying technologies/capabilities for MTC2 SOA.

3.1.1 The contractor shall perform daily system status and health checks for server management/processes and web service operation and availability.

3.1.2 The contractor shall troubleshoot and work to resolve server operational anomalies.

3.2 The contractor shall perform software installation, administration and configuration for MTC2 SOA and its components. The contractor shall monitor server operating system and web server logs and research and resolve log issues and anomalies. The contractor shall perform web application testing, trouble-shooting and application configuration on different network environments to ensure maximum functionality and compatibility and mitigate any limiting factors or negative impact to web applications.The contractor shall perform web server performance analysis, tuning and enhancements to maximize web application services, manage widgets and configure appropriately within system(s) boundaries.

3.2.1 The contractor shall perform web server Security Compliance utilizing the Information Assurance Support Environment Security Technical Implementation Guides (STIG) and Security References Guides applicable to system. The contractor shall provide Cyber Security Liasion (CSL) Customer Support by assisting customers with account issues. Cyber Security Workforce (CSWF) certification required as per section 7.6.

3.2.2 The contractor shall perform daily operational status checks and configurations for web applications. The contractor shall assist staff with configuration and effective use of web applications on multiple domains. The contractor shall assist CPF/C6F System Administration with maintaining web application suite operational capabilities. The contractor shall develop and manage server/application backup and disaster recovery plan. Provide internal weekly status to SSC Pacific MTC2 SOA leadership.

3.2.3 The contractor shall complete a Contractor’s Progress, Status and Management Report monthly **(CDRL A001)** covering all of the above tasks. The contractor shall immediately notify the Technical Coordinator and the COR if it identifies problems that may negatively impact completion of this SOW including schedule, cost, quality and rework issues.

3.2.4 Normal work schedule is 9 hours daily (1 hour lunch) - 40 hours weekly (M-F): Between the hours 0600 - 1730. The contractor shall provide emergent support in response to off-duty calls. The contractor shall provide on-site support as defined by the sponsor Program

Office 150 (PMW150), CPF and C6F. The contractor shall provide 24/7 support, as required, during exercises, operations and contingencies which may require 120-160 hours of rotational shift work during these situations.

4.0 OPTION PERIOD REQUIREMENTS: The option period requirements 4.1 through 4.2 are identical to the base period requirements as reflected above.

4.0 GOVERNMENT FURNISHED PROPERTY

4.1 None anticipated for this effort

5.0 CONTACTOR FURNISHED MATERIAL

5.1 None anticipated for this effort

6.0 TRAVEL

6.1 The following tavel is for estimating purposes only. All travel is expected to originate in the San Diego area. Contractors may propose alternated origins as required. It is anticipated that the following travel requirements may be necessary for Base and Option Year 1 (same locations, number of travelers, trips, days for base and option 1):

6.1.1 San Diego to Honolulu (CPF) – one (1) person, one (1) trip for seven (7) days.

6.1.2 San Diego to Italy (C6F) – one (1) person, one (1) trip for seven (7) days.

7.0 SECURITY

7.1 The work to be performed under this task shall be up to Top Secret level.

7.2 Anti-Terrorism/Force Protection (AT/FP) briefings are required for all personnel (Military, DOD Civilian, and contractor) per OPNAVINST F3300.53C. Contractor employees must receive the AT/FP briefing annually. The briefing is available at https://atlevel1.dtic.mil/at/, if experiencing problems accessing this website contact ssc_fortrav@navy.mil.

7.3 As required by National Industrial Security Program Operating Manual (NISPOM) Chapter 1, Section 3, contractors are required to report certain events that have an impact on: 1) the status of the facility clearance (FCL); 2) the status of an employee's personnel clearance (PCL); 3) the proper safeguarding of classified information; 4) or an indication that classified information has been lost or compromised. Contractors working under SSC Pacific contracts will ensure information pertaining to assigned contractor personnel are reported to the Contracting Officer Representative (COR)/Technical Point of Contact (TPOC), the Contracting Specialist, and the Security's COR in addition to notifying appropriate agencies such as Cognizant Security Agency (CSA), Cognizant Security Office (CSO), or Department Of Defense

Central Adjudication Facility (DODCAF) when that information relates to the denial, suspension, or revocation of a security clearance of any assigned personnel; any adverse information on an assigned employee's continued suitability for continued access to classified access; any instance of loss or compromise, or suspected loss or compromise, of classified information; actual, probable or possible espionage, sabotage, or subversive information; or any other circumstances of a security nature that would affect the contractor's operation while working under SSC Pacific contracts.

7.4 Secure Facility Open and Close Security. The contractor may be required to securely open and close designated SSC Pacific secure facilities in accordance with the latest SSC Pacific Instructions.

> 7.4.1 The contractor shall coordinate with the applicable facility manager in designating which contractor team members will be allowed opening and closing authority and will provide notification to that facility manager when changes occur.
>
> 7.4.2 The contractor shall ensure that all personnel granted opening and closing authority are properly trained for these duties and, if circumstances warrant, certified and/or designated by proper Government authority.
>
> 7.4.3 In accordance with SSCPACINST 2280.2C and SSC Pacific CMS Training Handbook, dtd April 2012, contractor team members with open and close authority in facilities operating and storing COMSEC equipment and materials shall achieve and maintain either CMS User or CMS Equipment Only Restricted Access Personnel (EORAP) User designation. In maintaining this designation, a contractor team member(s) will notify the Electronic Key Management System (EKMS) Manager, and 532 Lab Manager before departing on extended leave/TAD (in excess of 45 days), permanent detachment/departure, or of any changes in contractor team member work assignments that result in the termination of the need for access to CMS.

7.5 Operations Security: OPSEC is a five step analytical process (identify critical information; analyze the threat; analyze vulnerabilities; assess risk; develop countermeasures) that is used as a means to identify, control, and protect unclassified and unclassified sensitive information associated with U.S. national security related programs and activities. All personnel working under this task will at some time handle, produce or process Critical Information or CPI, and therefore all Contractor personnel must practice OPSEC. All work is to be performed in accordance with DoD OPSEC requirements, and in accordance with the OPSEC attachment to the DD254.

7.6 Cyber Security Workforce (CSWF) Workforce Requirements: The following CSWF categories, levels, training, and certifications are required for contractor personnel under this task order: Require a minimum of Information Assurance Technical (IAT) certification for client OS (e.g., Windows 10). All personnel installing, integrating, or requiring privileged access / system root access to server OSs require IAT Level II certifications for the respective operating system and environment (i.e. for Windows Operating System [Windows 7/Server 2008] and/or Unix Operating System (Red Hat Enterprise Linux [RHEL]) as appropriate.

The contractor shall ensure that personnel accessing information systems have the proper and current CSWF certification to perform IA functions identified in section 3.2 of this PWS in accordance with DoD 8570.01-M, Information Assurance Workforce Improvement Program. The contractor shall meet applicable CSWF certification requirements, including (a) DoD approved CSWF certifications appropriate for each specified category and level and (b) appropriate operating system certification for IA technical positions as required by DoD 8570.01-M. Contractor personnel who do not have proper and current certifications shall be denied access to DoD information systems for the purpose of performing IA functions.

The contractor shall provide documentation supporting the information assurance certification status of personnel performing information assurance functions, reporting current IA certification status and compliance using CDRL Contractor Roster (**A002)**, DI-MGMT-81596 in the format prescribed by the COR.

8.0 PLACE OF PERFORMANCE

8.1 Work on this task order will be performed at contractor site, on-site at (b)(3); (b)(7)(e)(f)